NOCIP

No Cloud Inference on Personal data

Audit Checklist

Version 1.0 · 2026-10-29 · Draft – not yet approved

This checklist is for be next GmbH's auditors. It is published so that applicants know what is tested. Every audit follows it in full; any deviation is explained in the audit report. Test data and canary values are not published.

1 Audit environment

- Test environment: the product runs on a NOCIP test machine or as test access. All traffic passes through an intercepting proxy (e.g. mitmproxy) with packet capture (all protocols, not only HTTP) and a DNS log.
- TLS: the audit certificate is installed. If certificate pinning prevents inspection, the vendor provides a test build without pinning or a log of outgoing data; otherwise the affected criteria count as not demonstrated.
- Canary values: new, unique canary values are generated for every audit, so that every match can be traced.
- Test corpus: the current version of the NOCIP test corpus (German and English) is used; the version is stated in the audit report.
- Retention: captures, logs and screenshots are kept for 3 years and not passed on.

Preparation

☐ Self-assessment complete, evidence available

☐ Test installation or test access set up

☐ Audit proxy, packet capture and DNS log running; audit certificate installed

☐ Canary value set generated for this audit (no. _____)

☐ Test corpus version noted (_____)

2 Audit per criterion

All tiers

C-01 Disclosure

Requirement	The product and the vendor's website state the NOCIP tier and say where AI processing takes place. Users can find this statement before first use (e.g. product page, settings, documentation).
Steps	☐ 1. Open the statements on the website and in the product. ☐ 2. Compare them with the architecture found in the audit.
Passed if	Statements present, accurate and matching the tier.
Result	☐ passed ☐ failed ☐ not applicable

Records	
Remark	

C-02 Model inventory

Requirement	The documentation lists every model used for the product's AI functions: name, version, licence, origin and where it runs (customer, vendor or third-party AI, with country).
Steps	☐ 1. Compare the inventory with installed model files, configuration and observed network traffic.
Passed if	Inventory complete and consistent.
Result	☐ passed ☐ failed ☐ not applicable
Records	
Remark	

C-03 No training on customer data

Requirement	Customer content is not used by the vendor or any third party to train or fine-tune models unless the customer explicitly opts in. Opt-in is off by default. Fine-tuning that takes place only on the customer's own systems is allowed.
Steps	☐ 1. Review the terms. ☐ 2. Check the product's default settings.
Passed if	No training without explicit opt-in; opt-in off by default.
Result	☐ passed ☐ failed ☐ not applicable
Records	
Remark	

C-04 No content in telemetry and logs

Requirement	Telemetry, usage statistics, crash reports and remote logs contain no document content, prompts, AI output or personal data taken from processed content.
Steps	☐ 1. Process test documents containing canary values. ☐ 2. Capture all outgoing traffic, including crash reports (trigger a crash where possible). ☐ 3. Search the capture for canary values.
Passed if	No canary value outside the transfers the tier allows.
Result	☐ passed ☐ failed ☐ not applicable
Records	
Remark	

C-05 Change notification

Requirement	The vendor reports changes to the AI architecture (new model or model provider, new processing location, new external connection, changed router or pseudonymisation) to NOCIP within 30 days. A change that leads to a lower tier is reported before it goes live.
Steps	☐ 1. Check the label agreement. ☐ 2. At spot checks and renewal: compare the architecture with the last audit report.
Passed if	Agreement signed; no unreported changes.
Result	☐ passed ☐ failed ☐ not applicable
Records	
Remark	

C-06 Connection list

Requirement	The vendor lists every outgoing network connection the product makes (destination, purpose, data sent). Processing the test documents creates no connections outside this list.
Steps	☐ 1. Run the product behind the audit proxy with packet capture. ☐ 2. Process the test corpus. ☐ 3. Compare observed connections and DNS queries with the list.
Passed if	No connection that is not on the list.
Result	☐ passed ☐ failed ☐ not applicable
Records	
Remark	

C-07 Data processing agreement

Requirement	If the vendor processes customer data (e.g. SaaS, remote support), it offers a data processing agreement under GDPR Art. 28 that names all sub-processors with access to AI input or output. Does not apply if the vendor receives no customer data.
Steps	☐ 1. Review the agreement and the list. ☐ 2. Compare the list with the model inventory and the connection list.
Passed if	Agreement available; list complete. Or: the vendor receives no customer data.
Result	☐ passed ☐ failed ☐ not applicable
Records	
Remark	

C-08 User-triggered reports

Requirement	If the product sends examples to the vendor at the user's request (e.g. to improve recognition), then only like this: (1) the user triggers each report, never automatically and never as a default. (2) The product first replaces personal data with invented data of the same format, without a mapping table. (3) A preview shows exactly what is sent, and the user can change it; words the user keeps in the original are confirmed once more before sending. (4) The vendor uses reports only to improve the product and does not pass them on. Does not apply if the product sends no reports.
Threshold	**Replaced: ≥ 99 % of structured identifiers (IBAN, e-mail, phone, ID and tax numbers), ≥ 98 % of person names and ≥ 95 % of all canary values – as B-03.**
Steps	☐ 1. Call the report function with texts of the test corpus. ☐ 2. Capture the reports sent, search them for canary values and compute the rates per group. ☐ 3. Check that nothing is sent without the user triggering it and that the preview matches what is sent. ☐ 4. Review the terms on how reports are used.
Passed if	All four conditions met and all three thresholds reached – or the product sends no reports.
Result	☐ passed ☐ failed ☐ not applicable
Measured value	DE: _____ EN: _____
Records	
Remark	

Gold

G-01 Local inference

Requirement	All inference for AI functions runs on the customer's devices or servers (own hardware, or a cloud environment the customer controls itself). No AI request goes to the vendor or to third parties.
Steps	☐ 1. Locate the installed model files. ☐ 2. Process the test corpus and capture the traffic. ☐ 3. Search the capture for canary values and AI requests.
Passed if	No AI request and no canary value in outgoing traffic.
Result	☐ passed ☐ failed ☐ not applicable
Records	
Remark	

G-02 Offline operation

Requirement	All AI functions work without an internet connection. Licence checks and updates are allowed if they carry no content and processing continues offline for at least 14 days.
Threshold	**Continued offline operation ≥ 14 days.**

Steps	☐ 1. Disconnect the network. ☐ 2. Process the test corpus with all AI functions. ☐ 3. Move the system clock forward 14 days, or verify the vendor's stated grace period.
Passed if	All AI functions work offline; grace period ≥ 14 days.
Result	☐ passed ☐ failed ☐ not applicable
Measured value	DE: _____ EN: _____
Records	
Remark	

G-03 Verifiable models

Requirement	Models and model updates are delivered as files with a published checksum or signature.
Steps	☐ 1. Recompute the checksum or verify the signature of a delivered model file.
Passed if	Checksum or signature matches.
Result	☐ passed ☐ failed ☐ not applicable
Records	
Remark	

Silver

S-01 Vendor-operated AI (Variant S-a)

Requirement	AI that processes personal data runs at the customer's site or on vendor-operated infrastructure in the EEA. No third-party AI sees personal data. A cloud provider's model services count as third-party AI.
Steps	☐ 1. Review hosting contracts and locations. ☐ 2. Obtain proof that the vendor runs the models itself (configuration, deployment, model files). ☐ 3. Process the test corpus through the service; check the vendor servers' outgoing traffic where accessible, otherwise the vendor's logs.
Passed if	Models demonstrably run at the vendor in the EEA; no third-party AI receives canary values.
Result	☐ passed ☐ failed ☐ not applicable
Records	
Remark	

S-02 Router (Variant S-b)

Requirement	If a third-party AI is used, a router at the customer's site or on vendor-operated infrastructure checks every request. Only requests without personal data go to the third-party AI.

Steps	☐ 1. Trace the router in the architecture. ☐ 2. Check that no request reaches the third-party AI bypassing the router.
Passed if	Every request to the third-party AI passes the router.
Result	☐ passed ☐ failed ☐ not applicable
Records	
Remark	

S-03 Router accuracy (Variant S-b)

Requirement	The router reliably keeps requests containing personal data away from the third-party AI.
Threshold	**Of the test requests containing personal data, at most 0.5 % reach the third-party AI (≥ 99.5 % kept back); for requests containing structured identifiers (IBAN, e-mail, phone, ID and tax numbers), at most 0.1 % (≥ 99.9 %).**
Steps	☐ 1. Send at least 1,000 test requests per language (mixed, with and without personal data). ☐ 2. Count which requests containing canary values reach the third-party AI. ☐ 3. Compute the rates separately for structured identifiers and other data.
Passed if	Both thresholds met, in German and in English.
Result	☐ passed ☐ failed ☐ not applicable
Measured value	DE: _____ EN: _____
Records	
Remark	

S-04 Router fails closed (Variant S-b)

Requirement	If the router is uncertain, fails or cannot be reached, the request stays local or with the vendor.
Steps	☐ 1. Deliberately disturb the router (stop it, force a timeout, return an invalid result). ☐ 2. Check whether any request reaches the third-party AI.
Passed if	Under no disturbance does a request reach the third-party AI.
Result	☐ passed ☐ failed ☐ not applicable
Records	
Remark	

Bronze

B-01 Pseudonymisation before transfer

Requirement	Every request to a third-party AI passes a pseudonymisation step at the customer's site or on vendor-operated infrastructure.
Steps	☐ 1. Trace the pseudonymisation step in the architecture. ☐ 2. Check that no request reaches the third-party AI bypassing it.

Passed if	Every request to the third-party AI is pseudonymised first.
Result	☐ passed ☐ failed ☐ not applicable
Records	
Remark	

B-02 Categories covered

Requirement	At least the following are covered: names of natural persons, addresses, dates of birth, phone numbers, e-mail addresses, IBAN and account numbers, ID card, passport, tax, social security and health insurance numbers, file and case reference numbers, vehicle registration numbers, IP addresses. The vendor lists any further categories.
Steps	☐ 1. Review the list. ☐ 2. Process canary values of each category in the test corpus (see B-03).
Passed if	All minimum categories covered.
Result	☐ passed ☐ failed ☐ not applicable
Records	
Remark	

B-03 Detection rate

Requirement	The pseudonymisation step reliably removes personal data. A canary value counts as leaked if it, or an obvious variant of its spelling, appears in plain text in the outgoing request.
Threshold	**Removed: ≥ 99 % of structured identifiers (IBAN, e-mail, phone, ID and tax numbers), ≥ 98 % of person names and ≥ 95 % of all canary values overall.**
Steps	☐ 1. Process at least 200 test documents per language. ☐ 2. Capture the outgoing requests to the third-party AI. ☐ 3. Determine for each canary value whether it appears in plain text; compute the rates per group.
Passed if	All three thresholds met, in German and in English.
Result	☐ passed ☐ failed ☐ not applicable
Measured value	DE: _____ EN: _____
Records	
Remark	

B-04 Mapping table stays

Requirement	The mapping table (placeholder ↔ real value) never leaves the customer or the vendor. Placeholders in AI output are replaced back at the customer's site or at the vendor.
Steps	☐ 1. Search outgoing requests for mappings (placeholder next to canary value).
Passed if	No mapping in outgoing traffic.
Result	☐ passed ☐ failed ☐ not applicable

Records	
Remark	

B-05 Pseudonymisation fails closed

Requirement	If pseudonymisation fails or cannot be reached, nothing is sent to the third-party AI.
Steps	☐ 1. Deliberately disturb the pseudonymisation (stop it, force a timeout, return an invalid result). ☐ 2. Check whether any request reaches the third-party AI.
Passed if	Under no disturbance does a request reach the third-party AI.
Result	☐ passed ☐ failed ☐ not applicable
Records	
Remark	

B-06 Visible to users

Requirement	Users can see what was sent to the third-party AI (preview before sending, or a log).
Steps	☐ 1. Open the preview or log in the product and compare it with the capture.
Passed if	Preview or log available and complete.
Result	☐ passed ☐ failed ☐ not applicable
Records	
Remark	

B-07 Contract with the third-party AI

Requirement	The contract with the third-party AI provider excludes training on the data, limits retention to at most 30 days, and provides for processing in the EEA or a valid basis for transfers to third countries.
Threshold	**Retention ≤ 30 days.**
Steps	☐ 1. Review the contract and configuration (region, retention).
Passed if	No training, retention ≤ 30 days, valid transfer basis.
Result	☐ passed ☐ failed ☐ not applicable
Measured value	DE: _____ EN: _____
Records	
Remark	

B-08 Correct wording

Requirement	The product and its marketing do not call pseudonymised data anonymous or anonymised.
Steps	☐ 1. Review product and marketing texts.
Passed if	Nothing described as anonymous.

Result	☐ passed ☐ failed ☐ not applicable
Records	
Remark	

3 NOCIP index

Within the tier, the NOCIP index rates the implementation with 0 to 10 whole points: five groups of 0 to 2 points each. The index never changes the tier; it is shown next to it (e.g. “Silver · 8/10”).

Group	1 point / 2 points	Points	Records
I-1 Transparency	1: A data-flow diagram is published that shows the processing location of every AI function. 2: In addition, the product shows for each AI function or request where it is processed.	☐ 0 ☐ 1 ☐ 2	
I-2 Customer control	1: The customer can switch off every external AI connection; the product then continues with reduced functions. (Gold: met.) 2: In addition, all AI functions are available in a variant that runs entirely at the customer's site. (Gold: met.)	☐ 0 ☐ 1 ☐ 2	
I-3 Data minimisation	1: AI input and output are kept outside the customer for at most 30 days. (Gold: met.) 2: In addition, nothing is kept outside the customer beyond processing, and local logs contain content only if the customer switches this on.	☐ 0 ☐ 1 ☐ 2	
I-4 Integrity	1: The product verifies the signature or checksum of every model before loading it. 2: In addition, local stores holding content or mapping tables are encrypted (or set-up with operating-system encryption is documented).	☐ 0 ☐ 1 ☐ 2	
I-5 Verifiability	1: The customer can view a log of all external AI requests (Gold: of all outgoing connections). 2: In addition, the vendor gives NOCIP permanent test access or a test installation for unannounced spot checks.	☐ 0 ☐ 1 ☐ 2	

4 Decision

1. Tier = highest tier whose criteria were all passed; all C criteria must be passed.
2. Silver: all criteria of the applicable variant(s) passed.
3. Index = sum of the five groups (0–10), stated only within the tier reached.
4. Failed criteria go into the audit report with a finding; offer one free retest.